

Role-based Access Control in SMW

SMWCon Fall 2013

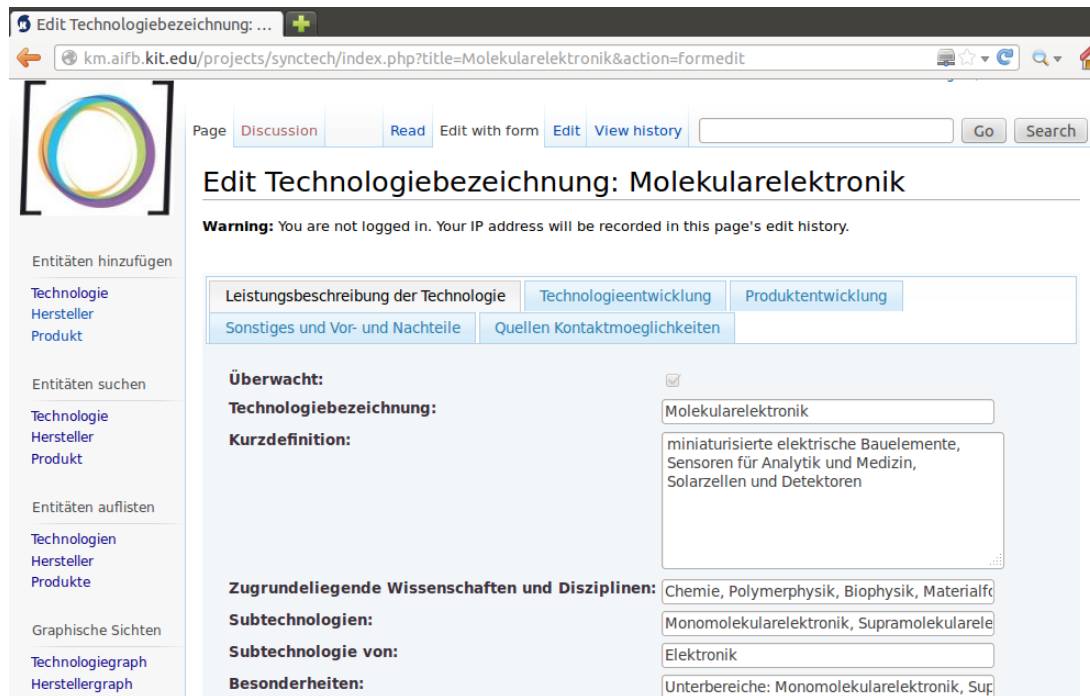
Wojtek Breiter, Michael Färber

Institut für Angewandte Informatik und Formale Beschreibungsverfahren (AIFB)



Access control as crucial point

- Semantic wikis as useful collaborative knowledge management tool in enterprises
- But: Associated with security concerns
- Example: Technology assessment for strategic focus



Edit Technologiebezeichnung: ...

km.aifb.kit.edu/projects/synctech/index.php?title=Molekularelektronik&action=formedit

Page [Discussion](#) [Read](#) [Edit with form](#) [Edit](#) [View history](#)

Edit Technologiebezeichnung: Molekularelektronik

Warning: You are not logged in. Your IP address will be recorded in this page's edit history.

Entitäten hinzufügen

Technologie
Hersteller
Produkt

Entitäten suchen

Technologie
Hersteller
Produkt

Entitäten auflisten

Technologien
Hersteller
Produkte

Graphische Sichten

Technologiegraph
Herstellergraph

Leistungsbeschreibung der Technologie **Technologieentwicklung** Produktentwicklung

Sonstiges und Vor- und Nachteile Quellen Kontaktmöglichkeiten

Überwacht: ☒

Technologiebezeichnung:

Kurzdefinition:

Zugrundeliegende Wissenschaften und Disziplinen:

Subtechnologien:

Subtechnologie von:

Besonderheiten:

Typical requirements for AC in enterprises' SMWs

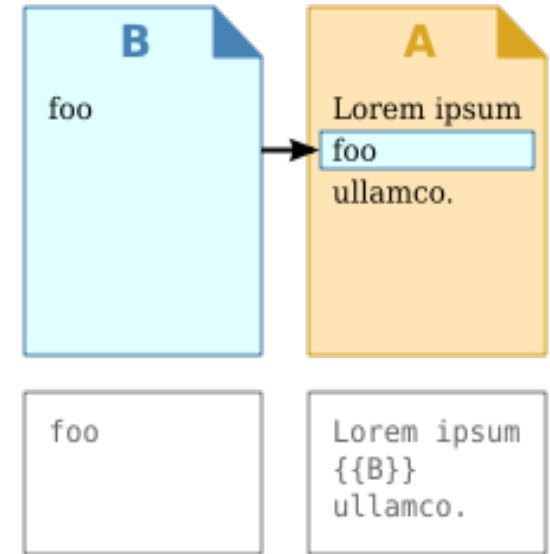
- User based and/or group based access control
 - Distinguish between read and edit access
 - Typical groups: Chairmen, department managers, employees
- AC protection for
 - Single pages
 - Namespaces
 - Semantic properties
- Secure
- AC plugin working with current MW / SMW versions
- Easy to use (adequate GUI)

Security issues with authorization extensions

Transclusion / Inclusion:

Access restricted pages by embedding restricted articles

→ Fixed with *\$wgNonIncludableNamespaces* setting since MW 1.10




- Preloading:

Circumvent the restriction using *editintro=* or *preload=* URI parameters in edit mode?


- XML/RDF export
- Atom/RSS Feed

→ All 3 issues solved using *userCan* hook
(since MW 1.12)

Mediawiki.org lists 12 extensions...

Extension	Pure extension	Works with caching	Works with MediaWiki groups	Page-based access control	Namespace-based access control
Extension:CrudeProtection	Yes	Yes	No (User Based)	Yes	No
Extension:Group Based Access Control	Yes	No	Yes	Yes	No
Extension:Halo Access Control List	No	Yes	Yes	Yes	Yes
IntraACL 	No	Yes	Yes	Yes	Yes
Extension:Lockdown	Yes	Yes	Yes	No	Yes
Extension:NSFileRepo	Yes	Yes	Yes	No	Yes
Extension:Page access restriction	No	No	Yes	Yes	Yes
Extension:PageProtectionPlus	Yes	No	Yes	Yes (really section based)	No
Extension:PageSecurity	No	No	Yes	Yes	No
Extension:PrivatePageProtection	Yes	Yes	Yes	Yes	No
Extension:Simple Security	Yes	No	Yes	Yes	Yes
Extension:WhiteList	Yes	Yes	No (user based)	Yes	No

...but:

Extension	Pure extension	Works with caching	Works with MediaWiki groups	Page-based access control	Namespace-based access control
Extension:CrudeProtection	Archieved				
Extension:Group Based Access Control	Archieved				
Extension:Halo Access Control List	No	Yes	Yes	Yes	Yes
IntraACL 	No	Yes	Yes	Yes	Yes
Extension:Lockdown	No single page protection				
Extension:NSFileDepo					
Extension:Page access restriction	Outdated				
Extension:PageProtectionPlus	No protection of NS				
Extension:PageSecurity	nor semantic properties				
Extension:PrivatePageProtection					
Extension:Simple_Security					
Extension:WhiteList	No group policy				

Only 2 candidates for our purpose remain from this list:

HaloACL and IntraACL

Plus 2 extensions (not mentioned in this list):

SemanticACL and SemanticAccessControl

Extension: Semantic Access Control

Pro:

- GUI to define User Groups
- Page specific AC through GUI
- AC statement can be embedded into template

Contra:

- no AC on properties

Usage for user AC:

```
{{ACL Page User Permission
|User={{PI}}}
Permission=read
|Grant=Grant
}}
```

For groups:

```
{{ACL Page Group Permission
|UserGroup=All Users
|Permission=write, read,
grant
|Grant=Reject
}}
```

Extension: Semantic Access Control

Pro:

- GUI to define User Groups
- Page specific AC through GUI
- AC statement can be embedded into template

Contra:

- no AC on properties

Usage for user AC:

```
{{ACL Page User Permission  
|User={{PI}}}  
Permission=read  
|Grant=Grant  
}}
```

For groups:

```
{{ACL Page Group Permission  
|UserGroup=All Users  
|Permission=write, read,  
grant  
|Grant=Reject  
}}
```

Extension: SemanticACL

Pro:

- supports AC on properties
- works with current versions

Contra:

- only prevents direct views
- no special site to administrate
- no GUI

Usage examples:

```
[[Visible to  
group::moderator]]
```

```
[[Editable by  
user::User:Chief Moderator]]
```

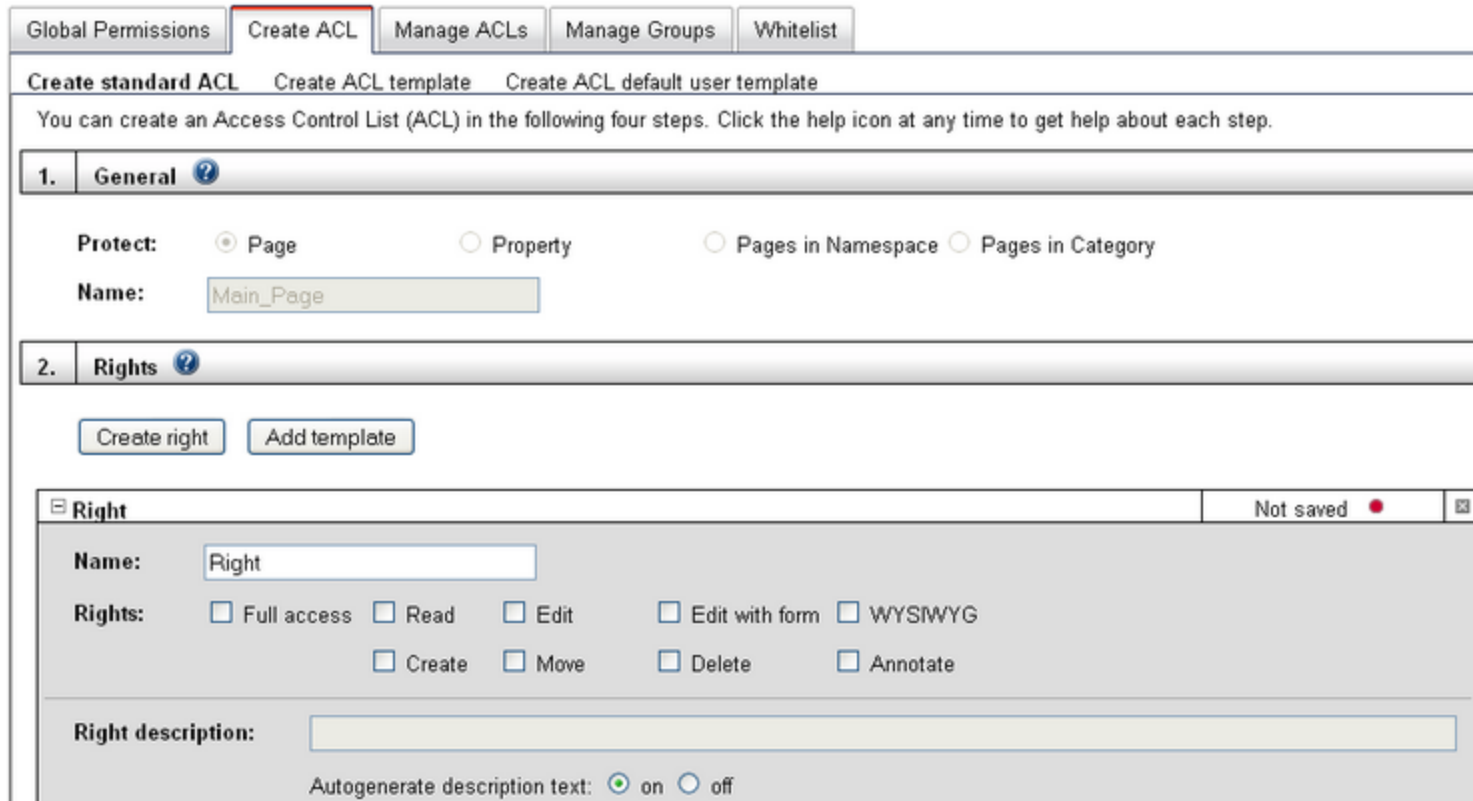
Extension:Halo Access Control List

Pro:

- Protection of categories, namespaces and single pages
- Protection of properties

Contra:

- Supports MW 1.13 – 1.17
- SMW 1.4.2 – 1.7.1
- Depending on further extensions



Global Permissions **Create ACL** Manage ACLs Manage Groups Whitelist

Create standard ACL Create ACL template Create ACL default user template

You can create an Access Control List (ACL) in the following four steps. Click the help icon at any time to get help about each step.

1. General ?

Protect: ☒ Page ☐ Property ☐ Pages in Namespace ☐ Pages in Category

Name:

2. Rights ?

Create right Add template

Right Not saved

Name:

Rights: ☐ Full access ☐ Read ☐ Edit ☐ Edit with form ☐ WYSIWYG ☐ Create ☐ Move ☐ Delete ☐ Annotate

Right description:

Autogenerate description text: ☒ on ☐ off

Extension: IntraACL

Pro:

- Based on HaloACL
- Eliminated some flaws and bugs
- Works on current versions
- GUI
- Easy to install
- Easy to use

Contra:

- No AC for properties

Conclusion

	GUI	User/Groups	Pages/NS	Properties	Special Admin Site	Up-to-date
HaloACL	✓	✓ / ✓	✓ / ✓	✓	✓	✗
IntraACL	✓	✓ / ✓	✓ / ✓	✗	✓	✓
SemanticAC	✗	✓ / ✓	✓ / ✓	✗	✗	✓
SemanticACL	✓	✓ / ✓	✓ / ✓	✗	✗	✓

→ no perfect solution!

Our approach:

- Update HaloACL for current MW and SMW versions

Thank you!